Lockheed Martin
Cyber Resiliency Level® (CRL®) Framework V3.0
for Weapon, Mission, and Training Systems

Dr. Dawn Beyer, Sr. Fellow; Dr. Michael Nance, Sr. Fellow; Patrick Lardieri, Sr. Fellow;
Nelson Roberts, Fellow; Rob Hale, Fellow; Tom Plummer, Fellow; and John Johnson II, Fellow
Lockheed Martin Corporation

As weapon systems[1] have become more dependent on globally-sourced embedded technology, software, and interconnected networks, new cyber risks continue to emerge. In order for weapon systems to successfully conduct their missions in cyber-contested environments[2], these risks must be identified and effectively managed (Government Accountability Office [GAO], 2018). The deficiency in risk awareness and management, coupled with rapid technology changes within complex environments that are continuously under attack, make measuring cyber resiliency a hard problem. Lockheed Martin (LM) Fellows and cybersecurity subject matter experts from across the corporation developed and piloted the Cyber Resiliency Level® (CRL®) Framework as a standard way to measure the cyber resiliency maturity of weapon systems. The CRL Framework can be used to assist stakeholders in prioritizing risks and selecting courses of action for maximum effect against cyber attacks, as well as provide stakeholders with an understanding of cyber investments necessary for increased cyber resilience.

Background

LM Fellows developed and continue to refine a method that enables programs to employ common risk- and engineering-based approaches to measure the cyber resiliency of weapon systems.

The team first developed a standard definition for the term *cyber resiliency*. With so many definitions already in existence, the Fellows combined three familiar, working definitions to establish the following description: *"Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to changing conditions to maintain the functions necessary for mission effective capability"* (Air Force [AF], 2017; Chairman of the Joint Chiefs of Staff [CJCS], 2018; National Institute of Standards and Technology [NIST], 2019).

After identifying the problem and defining the term, the following project objectives were determined:

1. Research and categorize top cyber concerns of the Department of Defense (DoD) (six CRL categories).

[1] The term 'weapon systems' is used to refer to major acquisition programs. These include a broad range of systems such as aircraft, missiles, ships, combat vehicles, radios, sensors, and satellites as well as their associated ground systems, simulators and training systems (GAO, 2018).

[2] A 'cyber contested environment' is when one or more adversaries attempt to change the outcome of a mission by denying, degrading, disrupting, or destroying our cyber capabilities, or by altering the usage, product, or our confidence in those capabilities (GAO, 2018).

2. Develop a conceptual model (CRL Framework; see Figure 1) and describe the categories, levels, and criteria (CRL Guidebooks).
3. Identify and define levels of increasing resiliency (CRL maturity level descriptions; see Figure 2).
4. Identify the qualitative and quantitative cyber performance measures for each category level (Cyber Resiliency Scoreboard (CRS)).

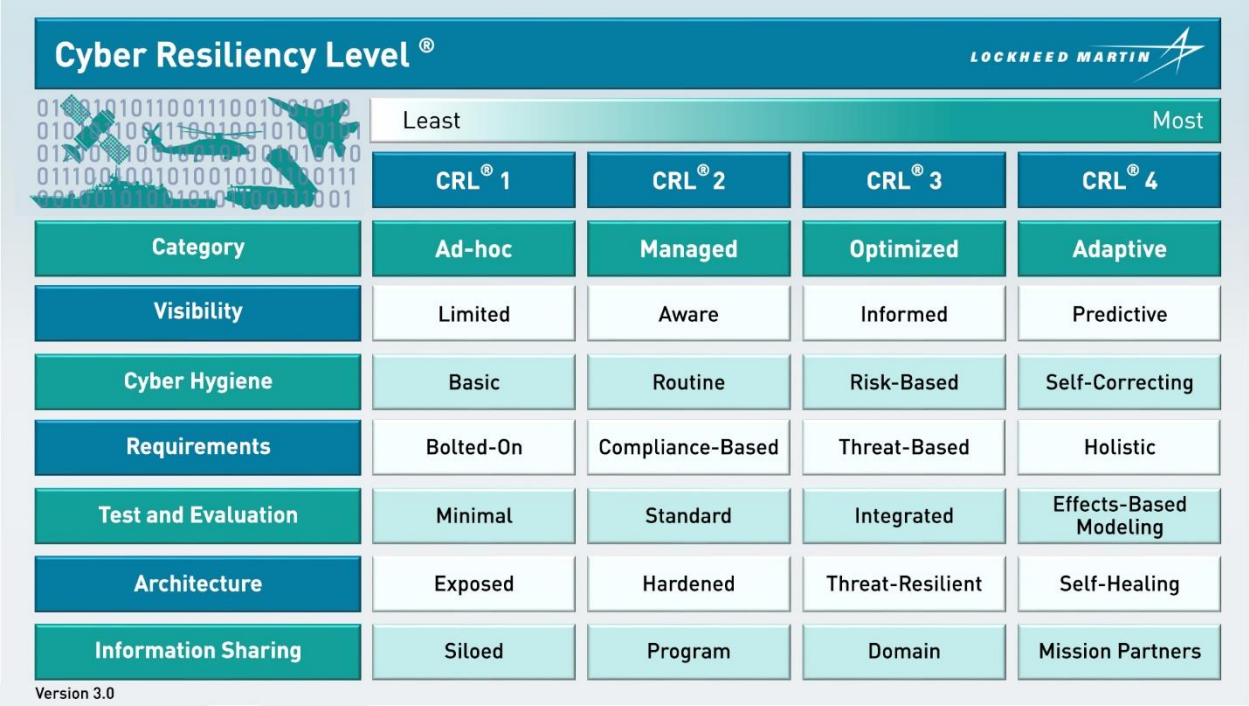

Figure 1. Cyber Resiliency Level® Framework V3.0

Overview

The CRL includes the framework (see Figure 1), guidebooks, maturity levels and descriptions (see Figure 2), and the CRS which contribute to the evaluation of resiliency across six categories. These six categories form the major recurring concerns of the DoD and were pulled from across their strategy, policies, practices, testimonies, and conference proceedings. An overview of each category is provided below:

1. **Visibility –** ability to sense, collect, and fuse data to inform defense and response
2. **Cyber Hygiene –** ability to manage the most common and pervasive cyber risks throughout the life cycle
3. **Requirements –** ability to identify, analyze, and define specifications commensurate with mission importance, risk, and the operational environment
4. **Test and Evaluation –** ability to measure the effectiveness of controls against mission objectives
5. **Architecture –** ability to maintain capability against cyber attacks

6. **Information Sharing –** ability to share timely cyber threat information and defensive measures to improve the cyber defensive posture

Each category is split into four levels of increasing maturity: CRL 1 – Ad-hoc, CRL 2 – Managed, CRL 3 – Optimized, and CRL 4 – Adaptive (see Figure 2).

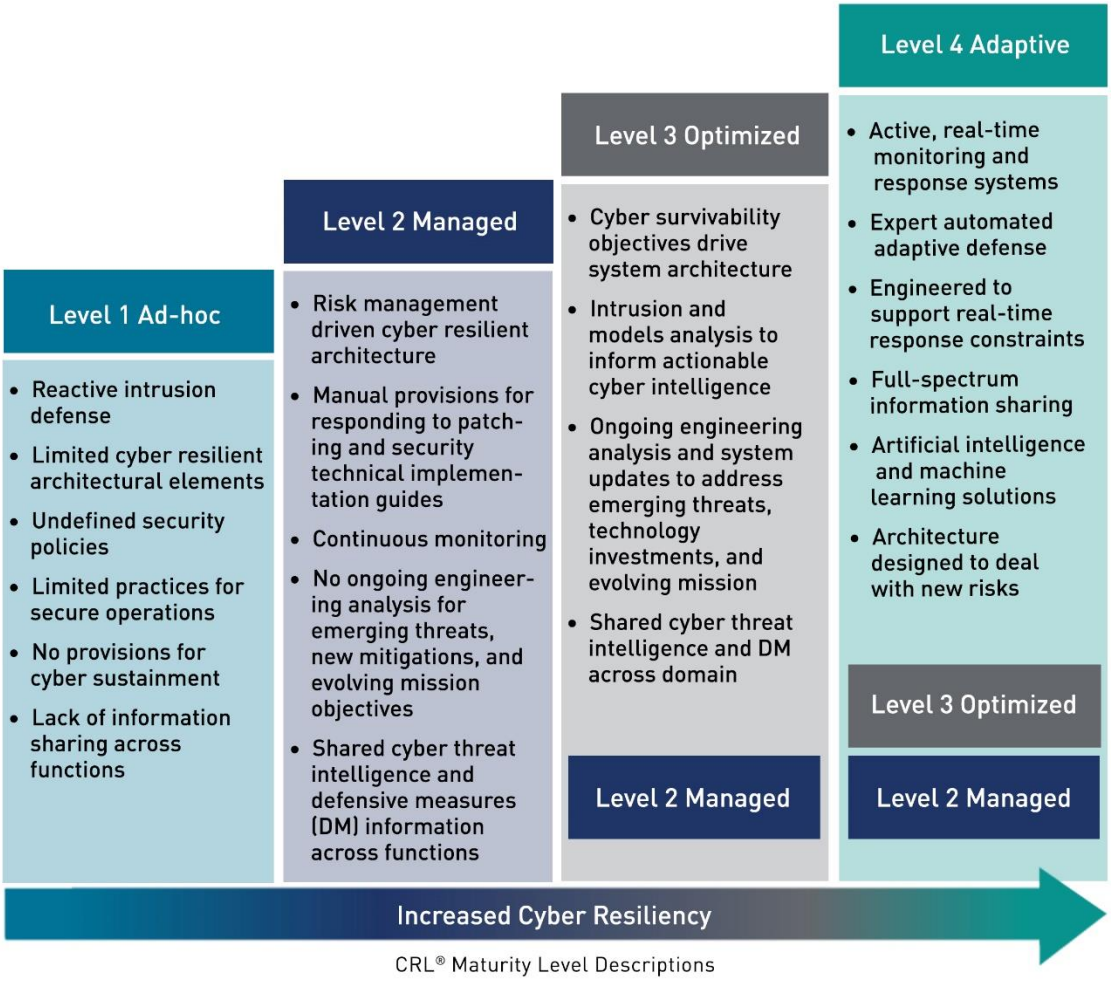

Figure 2. CRL® maturity level descriptions

Usage

The CRL can be used in any phase of the acquisition life cycle, concept to sunset, and—depending on the scope of the assessment—in any environment, such as development, manufacturing, operations, and supply chain. The processes and practices to perform each step are specified in the guidebooks and the CRS.

The CRL embraces the following four steps (Defense Science Board [DSB], 2016):

1. Identify level of cyber resiliency that currently exists and/or is planned.
2. Assess cyber risk.

3. Identify relationships between cyber investments and amount of increased resilience to attack.
4. Prioritize recommendations for cyber investment.

Step 1: Identify level of cyber resiliency that currently exists and/or is planned.

The purpose of this step is to leverage the criteria outlined in the guidebooks and the performance measures delineated in the CRS to evaluate the CRL of the weapon system. The CRS is a measurement tool which consists of a questionnaire and dashboard. The questionnaire provides qualitative and quantitative cyber performance measures based on category criteria. The questionnaire responses are used for the back-end analysis and represented via a dashboard. The dashboard consists of data sets and graphs that can be leveraged to assist stakeholders in measuring the resiliency that currently exists and/or is planned.

Requirements and/or controls are correlated to a category and evaluated against category criteria and performance measures. A CRL measurement is provided for each individual category. The resulting measurement of categories is expressed using a radar chart (see Figure 3). Results from this step give stakeholders improved insight into the level of cyber resiliency that currently exists and/or is planned.

Figure 3. CRL® – Step 1

Determining what products provide useful data to measure the CRL in Step 1 depends on the phase, within the acquisition cycle, the team is in at the time of assessment. For example, if the team is in the proposal phase, they can use the requirements outlined in the statement of work; if in planning, the team can utilize the concept of operations; if in development, the team can leverage the requirements and design documents; if in operations, the team can assess controls called out in engineering and system documentation, existing risk matrices, and assessment results.

Step 2: Assess cyber risk.

The purpose of this step is to assess the overall risk of the weapon system. Step 1 measures overall cyber resiliency mechanisms in place. Step 2 uses that information in combination with information from other sources and assessment methods to perform a risk assessment. The assessment step is used to identify, analyze, and prioritize risk (NIST, 2011). The team should leverage stakeholders' input in prioritizing risk.

To perform Step 2, the CRL endorses multiple assessment methods including NIST's Risk Management Process, DoD's Cyber Table Top (CTT), LM's Intelligence Driven Defense®, penetration testing, vulnerability scans, etc. In the example outlined in Figure 6, DoD's CTT is used.

Figure 4. CRL® – Step 2

Step 3: Identify relationships between cyber investments and amount of increased resilience to attack.

The purpose of this step is for stakeholders to use prioritized risks to identify and evaluate courses of action (CoA) (NIST, 2011). The CRS and the processes outlined in the guidebooks are used to identify and evaluate candidate CoAs. A cost-benefit analysis is performed to estimate CoA strengths and weaknesses to determine which CoA will provide the best approach to achieving estimated benefits, preserving cost, and mitigating risks while increasing resiliency (see Figure 5).

Figure 5. CRL® – Step 3

Step 4: Prioritize recommendations for cyber investment.

In Step 4, the evaluation team collaborates with stakeholders to prioritize and select CoAs. The team compares selected CoAs to the criteria delineated in the CRS to identify category levels. Results are presented to stakeholders via a radar chart (see Figure 6) to provide visualization comparison between as-is results and to-be recommendations.

Figure 6. CRL® – Step 4

CoAs then transition into controls that are defined by requirements and architecture concepts. Leveraging existing systems' engineering and risk management processes, controls along with cost/benefit analysis, schedule, and technical baseline impacts are reviewed and approved by stakeholders. From design through test, the selected controls are integrated into the technical solution and corresponding requirements are verified.

Repeat Step 2 (as required):

After controls are integrated into the operational environment, stakeholders can decide to do another assessment (see Figure 7) to validate the effectiveness of controls and leverage the radar chart, for the third time, to display the actual level of protection.

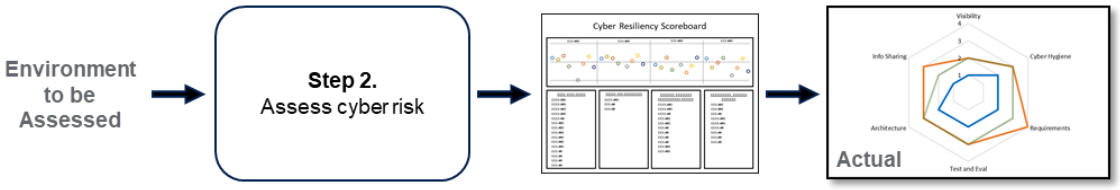

Figure 7. CRL® – Repeat Step 2

LM CRL and DoD CMMC

The LM CRL and the DoD's Cybersecurity Maturity Model Certification (CMMC) are independent with different purposes yet complement each other when assessing tactical to strategic risk. The CRL focuses on weapon systems to include the related equipment, materials, services, personnel, and means of delivery and deployment required for self sufficiency. The CMMC focuses on cybersecurity assessment of enterprise networks and Controlled Unclassified Information as it flows throughout program multitiered supply chains. Both the CRL and CMMC, when leveraged together, can provide a multitiered (organization, mission/business, and information system) risk management approach.

Summary

The Lockheed Martin Cyber Resiliency Level® (CRL®) Framework is used to measure the cyber resiliency maturity of a weapon system. CRL can be leveraged in any phase of the acquisition life cycle and—depending on the scope of the assessment—in any environment, such as development, manufacturing, operations, and supply chain. The CRL allows stakeholders to prioritize and select solutions for maximum effect against cyber attacks and provides stakeholders with an understanding of cyber investments necessary for increased cyber resilience. CRL products include a structured framework (see Figure 1), maturity levels and descriptions (see Figure 2), guidebooks, and the CRS.

Since 2018, the project team has used new research, lessons learned, and stakeholder feedback from several program pilots and customer engagements across all business areas to build and transform CRL artifacts. Recent changes included updates to the Framework and the Criteria, Measures, and Measurements (CMM) workbook. Within the Framework, version 3.0, the Architecture category (see Figure 1) levels were changed to: CRL 1 – Exposed, CRL 2 – Hardened, CRL 3 – Threat-Resilient, and CRL 4 – Self-Healing. The CMM workbook transitioned to the CRS, which streamlined the measurement process by making it more simplistic, understandable, and easier to discuss with stakeholders.

LM continues to collect, assess, and disposition program feedback to mature the framework, guidebooks, and CRS, and to shape processes, practices, and training.

Acknowledgements

LM Fellows, Rising Technical Talent, and the Cyber Senior Advisory Board provided valuable subject matter expertise, guidance, and leadership. The CRL Category Leads, CRL Change Control Board, Program Stakeholders, and the CRS product team provided significant contributions to CRL Version 3.0. The CRL Architecture category level changes were led by Ethan Puchaty. The CMM workbook to CRS transformation was led by Jacquelyn Blanchard and Orion Strimenos.

References

AF. (2017). *Cyber Resiliency Office for Weapon Systems briefing.*

CJCS. (2018). *Joint Publication 3-14. Space Operations.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf

DSB. (2016). *DSB Task Force Report on Cyber Defense Management.* https://apps.dtic.mil/dtic/tr/fulltext/u2/1023639.pdf

GAO. (2018). *GAO-19-128: Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities.* https://www.gao.gov/assets/700/694913.pdf

NIST. (2011). *NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST. (2019). *NIST SP 800-160V2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf